JO-FinCERT – Security Advisory – 2023 – 41

1. Cisco fixes AnyConnect bug giving Windows SYSTEM privileges

Cisco has addressed a high-severity vulnerability tracked as (CVE-2023-20178) in their Cisco Secure Client (formerly AnyConnect Secure Mobility Client) software, which could allow low-privileged, local attackers to escalate their privileges to the operating system's SYSTEM account. Cisco Secure Client is utilized for secure remote work via a Virtual Private Network (VPN) and offers endpoint management and telemetry features. The flow can be exploited through low-complexity attacks that don't require user interaction.

Recommendations: Cisco has released a fix for this vulnerability, and users are strongly advised to update their Cisco Secure Client software to the latest version to ensure protection against potential attacks.

- **CVE-2023-20178**: The vulnerability allows a local user to escalate privileges on the system.

Reference: https://www.bleepingcomputer.com/news/security/cisco-fixes-anyconnect-bug-giving-windows-system-privileges/

2. VMware fixes critical vulnerabilities in vRealize network analytics tool

VMware has released several security patches to resolve critical and high-severity vulnerabilities in VMware Aria Operations for Networks. These vulnerabilities enable attackers to remotely execute malicious code or gain unauthorized access to sensitive information. Formerly known as vRealize Network Insight (vRNI), this tool is utilized by administrators to enhance network performance, manage VMware and Kubernetes deployments, and leverage network visibility and analytics features.

Recommendations: Applying the provided security patches to mitigate the risk associated with these vulnerabilities, and ensure the secure operation of their VMware Aria Operations for Networks installations.

- **CVE-2023-20888 / CVE-2023-20887 / CVE-2023-20889:** Enables malicious actors to access sensitive information following a successful command injection attack.

Reference: https://www.vmware.com/security/advisories/VMSA-2023-0012.html

3. CEO guilty of selling counterfeit Cisco devices to military, govt orgs

Barracuda, an email and network security company, has issued a warning to its customers regarding the need to replace their Email Security Gateway (ESG) appliances. This action is necessary due to recent attacks that targeted a zero-day vulnerability, which has since been patched.

Recommendations: Barracuda emphasized that affected ESG appliances must be replaced immediately, regardless of the patch version level. This measure is crucial to ensure the continued security and protection of customer systems and data.

- **CVE-2023-2868:** A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product effecting versions 5.1.3.001-9.2.0.006. CVSS 9.8/CRITICAL
-

Reference: https://www.barracuda.com/company/legal/esg-vulnerability